Версия 1

ДЗЕТА-ФУНКЦИЯ. ОТ ЭЙЛЕРА ДО ГИПОТЕЗЫ БЕРЧА И СВИННЕРТОН-ДАЙЕРА

Этот текст находится в состоянии постоянного изменения и улучшения. Когда-нибудь он станет частью книжки и перестанет меняться, а пока что пожелания по улучшению его математического содержания всячески приветствуются.

1. Занятие 1. Дзета-функция Римана.

Определение 1. Пусть s — действительное число. Тогда

(1) $$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Теорема 1. *Ряд* (1) *сходится при* $s > 1$ *и расходится при* $s \leq 1$.

Таким образом формула (1) определяет Дзета-функцию при $s > 1$. Нетрудно видеть, что эта функция бесконечно дифференцируема и $\lim_{s\to 1} \zeta(s) = \infty$. Позднее мы увидим, что можно определить Дзета-функцию при $s < 1$, и даже при всех комплексных $s \neq 1$.

Вот общий факт, на котором было основано доказательство теоремы 1:

Задача 1. Пусть a_n — невозрастающая последовательность. Докажите, что ряд $\sum a_n$ сходится тогда и только тогда, когда ряд $\sum 2^n a_{2^n}$ сходится.

Насколько быстро растут частичные суммы ряда (1), определяющего дзета функцию?

Задача 2. Обозначим $a_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ частичную сумму ряда (1) при $s = 1$. Докажите, что $\ln(n+1) < a_n \leq 1 + \ln n$. Найдите аналогичные оценки для частичных сумм ряда (1) при других значениях s. (Указание: сравните a_n с $\int_1^n \frac{dx}{x}$.)

1.1. Значения Дзета-функции.

Вычислить значение Дзета-функции хотя бы в одной точке — совсем не тривиальная задача. Вот что известно в этом направлении:

- (2) $$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} + \ldots = \frac{\pi^2}{6}.$$
  Задача вычисления $\zeta(2)$ известна как *проблема Базеля*. Она была решена Эйлером в 1935-м году. Впрочем, его доказательство было нестрогим. Мы приведем два доказательства в параграфе 1.3 (одно из них строгое).
- $\zeta(4) = \pi^4/90$.
- Вообще

(3) $$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{2(2n)!},$$

где B_{2n} — *число Бернулли* с номером $2n$. Числа Бернулли определяются следующей формулой:

(4)
$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}.$$

Мы приведем набросок доказательства в разделе 1.3.

- Точные формулы для значений ζ в нечетных натуральных числах неизвестны. Однако Апери доказал в 1978 году, что $\zeta(3)$ иррационально.
- В 2001 году Вадим Зудилин доказал, что среди чисел $\zeta(2n+1)$ бесконечно много иррациональных.
- Он также доказал, что хотя бы одно из чисел $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ иррационально.

1.2. **Произведение Эйлера.** Исключительная важность Дзета-функции Римана для теории чисел во многом связана с ее разложением в бесконечное произведение (5), к которому мы переходим. Заметим, что существенная часть этой брошюры посвящена обобщениям и применениям таких разложений.

Начнем с определений. Пусть a_n — бесконечная числовая последовательность. По аналогии с суммой ряда, можно определить бесконечное произведение. Для этого рассмотрим последовательность $b_n = a_1 a_2 \dots a_n$. *Бесконечным произведением*

$$\prod_{n=1}^{\infty} a_n$$

называется $\lim_{n\to\infty} b_n$. Говорят, что произведение *сходится*, если этот предел конечен и *отличен от нуля.*

Задача 3. Вычислите

$$\prod_{n=2}^{\infty} \left(1 - \frac{1}{n}\right) \quad \text{и} \quad \prod_{n=2}^{\infty} \left(1 - \frac{1}{n^2}\right).$$

Связь Дзета-функции с теорией чисел основана на следующей формуле:

Теорема 2 (Произведение Эйлера)**.**

(5)
$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

где произведение берется по всем простым числам. Более того, левая часть сходится тогда и только тогда, когда сходится правая часть.

В частности, взяв $s = 1$, получим

(6)
$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\dots\left(1 - \frac{1}{p}\right)\dots = 0.$$

Следствие 2.1. *Существует бесконечно много простых чисел.*

Следствие 2.2. *Имеем*

$$\sum \frac{1}{p} = \infty,$$

где сумма берется по всем простым числам.

Этот результат кажется удивительным — ведь простых чисел так мало!

Задача 4. Докажите, что найдется такая константа $C > 0$, что для всех n

$$\sum_{p<n} \frac{1}{p} > C \ln(\ln n). \tag{7}$$

Замечание 1. Обозначим левую часть (7) через a_n. Можно показать, что

$$\lim_{n\to\infty} \frac{a_n}{\ln(\ln n)} = 1.$$

1.3. **Значения Дзета-функции в четных положительных целых числах.** Стандартное доказательство формул (2) и (3) основано на замечательной формуле Валлиса:

$$\frac{\sin x}{x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{\pi^2 n^2}\right). \tag{8}$$

Доказательство Эйлера выглядело следующим образом: Пусть $p(x)$ — многочлен степени n, имеющий n различных ненулевых корней $x_1, \dots, x_n$. Тогда мы можем записать:

(9)

$$p(x) = a(x - x_1)\dots(x - x_n) = (ax_1 \dots x_n)\left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right)\dots\left(1 - \frac{x}{x_n}\right) =$$
$$= p(0)\left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right)\dots\left(1 - \frac{x}{x_n}\right).$$

Применим эту формулу к “многочлену” $\sin x/x$ (который мы продолжим в ноль по непрерывности). Замечая, что его корни — это целые кратные π, а значение в нуле равно единице, получим

$$\frac{\sin x}{x} = \prod_{n>0}\left(1 - \frac{x}{\pi n}\right)\left(1 + \frac{x}{\pi n}\right) = \prod_{n>0}\left(1 - \frac{x^2}{\pi^2 n^2}\right).$$

Конечно, $\sin x/x$ — не многочлен, тем не менее этому доказательству можно придать смысл, если использовать комплексный анализ. Мы дадим набросок доказательства в приложении...

Теперь докажем формулу (2). Разложим обе части формулы Валлиса с ряд Тейлора с точностью до членов малых по сравнению с x^2. Имеем

$$1 - \frac{x^2}{6} + \ldots = 1 - \left(\sum_{n=1}^{\infty} \frac{1}{\pi^2 n^2} \right) x^2 + \ldots$$

Приравнивая коэффициенты при x^2, получаем:

$$\frac{-1}{6} = -\sum_{n=1}^{\infty} \frac{1}{\pi^2 n^2},$$

откуда и следует искомая формула. Мы приведем элементарное доказательство формулы (2) чуть ниже.

Задача 5. Выведите формулу (3) из формулы Валлиса. (Указание:

$$(\ln(\sin x))' = \cot x = i + \frac{2i}{e^{2ix} - 1},$$

где $i = \sqrt{-1}$.)

Задача 6. Вычислите B_0, B_1, B_2, B_4, B_6. Докажите, что $B_{2k+1} = 0$ при $k \geq 1$.

Оказывается числа Бернулли возникают из следующей естественной задачи. При $k \geq 0$ определим

$$S_k(n) = 1^k + 2^k + \ldots + n^k.$$

Например, $S_0(n) = n$, $S_1(n) = n(n+1)/2$, $S_2(n) = n(n+1)(2n+1)/6$. Возникает гипотеза, что $S_k(n)$ — многочлен степени $k+1$ от n. Ответ дается следующей задачей.

Задача 7. Докажите, что

$$S_k(n) = \frac{1}{k+1} \sum_{j=0}^{k} (-1)^j \binom{k+1}{j} B_j n^{k+1-j}.$$

(Указание: Вычислите $\sum_{k=0}^{\infty} S_k(n) \frac{t^k}{k!}$.)

А теперь мы приведем строгое решение проблемы Базеля

Теорема 3.

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Доказательство. Зафиксируем нечетное число $n = 2m+1$. Положим $a_r = \pi r/n$, где $1 \leq r \leq m$. Ясно, что

$$S_m = \sum_{r=1}^{m} \frac{1}{a_r^2} = \frac{n^2}{\pi^2} \sum_{r=1}^{m} \frac{1}{r}^2. \tag{10}$$

Поэтому достаточно доказать, что $S_m/(2m+1)^2$ стремится к $1/6$, когда m стремится к бесконечности. Заметим, что

$$\sin a_r < a_r < \tan a_r$$

(это верно для любого числа на интервале $(0;\pi/2)$). Поэтому

$$x_r < \frac{1}{a_r^2} < y_r, \tag{11}$$

где $x_r = \dfrac{\cos^2 a_r}{\sin^2 a_r}$, $y_r = \dfrac{1}{\sin^2 a_r}$. Положим $X_m = \sum_{r=1}^m x_r$, $Y_m = \sum_{r=1}^m y_r$, имеем

$$X_m < S_m < Y_m.$$

Заметим, что $y_r - x_r = 1$, поэтому $Y_m - X_m = m$. Мы докажем, что

$$X_m = \frac{m(2m-1)}{3}. \tag{12}$$

Тогда

$$\lim_{r\to\infty} \frac{X_m}{(2m+1)^2} = \lim_{r\to\infty} \frac{Y_m}{(2m+1)^2} = \frac{1}{6}$$

и наше утверждение следует из принципа двух милиционеров. Итак, осталось доказать (12). Имеем

$$\sin nx = \mathrm{Im}(\cos x + i\sin x)^n = \binom{n}{1}\sin x\cos^{n-1}x - \binom{n}{3}\sin^3 x\cos^{n-3}x + \ldots$$

Деля на $\sin^n x$, получим

$$\frac{\sin nx}{\sin^n x} = \binom{n}{1}\cot^{n-1}x - \binom{n}{3}\cot^{n-3}x + \ldots = p_m(\cot^2 x),$$

где p_m — некоторый многочлен степени m. Ясно, что $p_m(x_r) = 0$. Значит, $x_1, \ldots, x_m$ — в точности корни многочлена p_m. По теореме Виета их сумма равна $\binom{n}{3}\big/\binom{n}{1}$, что совпадает с (12). □

1.4. **Вероятность выбора взаимно-простых чисел.** Пусть из отрезка $[1;N]$ случайно выбираются k целых чисел. Обозначим через $p_k(N)$ вероятность того, что эти числа взаимно просты в совокупности. Иными словами, пусть $P_k(N)$ есть число наборов из k взаимно простых чисел, лежащих на этом отрезке. Тогда $p_k(N) = P_k(N)/N^k$. Число $p_k = \lim_{N\to\infty} p_k(N)$ естественно считать вероятностью того, что k случайно выбранных чисел взаимно просты в совокупности

Теорема 4.

$$p_k = \zeta(k)^{-1}.$$

Следствие 4.1. *Два случайно выбранных натуральных числа взаимно просты с вероятностью* $6/\pi^2$.

Замечание 2. Имеется следующее рассуждение, которое, впрочем, мы не умеем делать строгим: вероятность того, что k случайных чисел не все делятся на два равна $1 - 2^{-k}$. Вероятность того, что не все числа делятся на три равна $1 - 3^{-k}$. Эти события независимы в силу китайской теоремы об остатках, так что вероятность того, что не все числа делятся на два *И* не все числа делятся на три равна $(1-2^{-k})(1-3^{-k})$. Продолжая в том же духе, видим что вероятность того, что числа не делятся все ни на одно простое, меньшее N, равна

$$\prod_{p<N}\left(1-\frac{1}{p^s}\right)$$

и в пределе мы получаем требуемое утверждение. К сожалению, выбор случайного натурального числа не имеет строго смысла.

Задача 8. Найдите такую функцию $\mu : \mathbb{Z} \to \mathbb{Z}$, что

$$\prod_{p}\left(1-\frac{1}{p^s}\right)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.$$

1.5. **Гипотеза Римана.** Невозможно говорить о Дзета-функции и не упомянуть о гипотезе Римана. Но для этого нужно сначала продолжить Дзета-функцию за пределы ее области сходимости. Сначала, мы выйдем в комплексную область

Задача 9. Докажите, что ряд (1) сходится при всех комплексных s из полуплоскости $\operatorname{Re} s > 1$.

1.5.1. *Аналитическое продолжение.*

Разминка 1. Положим

$$f(x) = 1 + x + x^2 + \ldots + x^n + \ldots$$

Нетрудно видеть, что $f(x)$ определена лишь при $|x| < 1$. Однако, если догадаться, что $f(x) = 1/1 - x$, то можно использовать эту формулу для продолжения $f(x)$ на $\mathbb{C} \setminus \{1\}$.

Это продолжение является “естественным”. Попытаемся придать точный смысл этим словам.

Пусть $U \subset \mathbb{C}$ — открытое множество. $f : U \to \mathbb{C}$ — функция. Напомним, что f называется *аналитической* или *голоморфной* в точке $z \in U$, если она может быть разложена в ряд в некоторой окрестности этой точки. Иными словами, если существует такое $r > 0$ и такие числа $a_n \in \mathbb{C}$, что

$$f(w) = \sum_{n=0}^{\infty} a_n (w-z)^n \text{ при } |w-z| < r. \tag{13}$$

Аналогичное определение можно дать для функции действительного переменного. В действительном случае, каждая аналитическая функция бесконечно

дифференцируема (то есть имеет производные всех порядков), но бывают не аналитические бесконечно дифференцируемые функции. В комплексном случае ситуация разительно отличается:

Факт 1. *Пусть* $f : U \to \mathbb{C}$ *дифференцируема на* U*, то есть в каждой точке* $z \in U$ *существует предел* $\lim_{w\to z} \frac{f(w)-f(z)}{w-z}$. *Тогда* f *имеет производные всех порядков на* U *и является аналитической функцией.*

Итак, пусть функция f аналитична в U. Возьмем $z \in U$ и разложим f в ряд в окрестности z. Пусть этот ряд сходится в круге $\{|w - z| < R\}$. Может так оказаться, что этот круг не содержится в U! Тогда мы продолжили нашу функцию на большее множество U'. Продолжая в том же духе, мы, при некотором везении, продолжим функцию на достаточно большое множество. Например, на $\mathbb{C}$ или на $\mathbb{C}$ без нескольких точек. Разумеется, так происходит не всегда. Нет никакого способа продолжить $\sqrt{z}$ на $\mathbb{C}$ без нескольких точек. Тем не менее, если для $f(z)$ такое продолжение существует, то оно *единственно* в силу следующей теоремы:

Теорема. *Пусть* f *и* g *голоморфные функции на* связном *открытом множестве* U*. Пусть* $A = \{z \in U : f(z) = g(z)\}$*. Если Множество* A *имеет предельную точку, то функции* f *и* g *совпадают на* U*.*

Мы докажем эту теорему в Приложении.

1.5.2. *Аналитическое продолжение Дзета-функции и гипотеза Римана.* Нетрудно видеть, что $\zeta(s)$ голоморфна при $\operatorname{Re} s > 1$ (см...). Оказывается, ее можно продолжить до функции, голоморфной во всех комплексных числах, кроме точки 1. Более того, оказывается существует простая связь между $\zeta(1 - s)$ и $\zeta(s)$:

Факт 2 (Функциональное уравнение для Дзета-функции)**.**

$$\zeta(1 - s) = \frac{2}{(2\pi)^s} \sin\left(\frac{\pi(1 - s)}{2}\right) \Gamma(s)\zeta(s),$$

где $\Gamma(s)$ *— Гамма-функция.*

Задача 10. Пусть нам удалось продолжить Дзета-функцию до функции, определенной при $\operatorname{Re} s > 0$ так, что при $0 < \operatorname{Re} s < 1$ выполняется функциональное уравнение. Докажите, что Дзета-функцию можно продолжить до аналитической функции, определенной при всех $s \neq 1$.

Попробуем найти все точки, где $\zeta(s) = 0$. Из произведения Эйлера следует, что $\zeta(s) \neq 0$ при $\operatorname{Re} s > 1$. С другой стороны, функциональное уравнение показывает, что при $\operatorname{Re} s < 0$ имеем

$$\zeta(s) = 0 \Longleftrightarrow s \in \{-2, -4, -6, \dots, -2n, \dots\}.$$

Задача 11. Докажите последнее утверждение. Указание: $\Gamma(s)$ не обращается в ноль при $\operatorname{Re} s > 0$.

Осталось выяснить, при каких s в полосе $0 < \operatorname{Re} s < 1$ Дзета-функция обращается в ноль...

Гипотеза Римана. Дзета-функция не обращается в ноль нигде, кроме точек $-2, -4, -6, \ldots$ и некоторых точек на прямой $\operatorname{Re} s = 1/2$.

2. Занятие 2. Дзета-функция кольца гауссовых чисел и представления натурального числа в виде суммы двух квадратов

На этом занятии мы будем изучать следующий вопрос: дано натуральное число n, можно ли его представить в виде суммы двух квадратов. Если можно, то сколькими способами?

2.1. Гауссовы числа.

Разминка 2. Число $n \in \mathbb{Z}$ можно представить в виде $x^2 - y^2$, где $x, y \in \mathbb{Z}$, если и только если $n \neq 4k + 2$.

Мы видим, что предыдущее диофантово уравнение решилось просто, потому что $x^2 - y^2$ можно разложить на множители. $x^2 + y^2$ тоже можно разложить на множители, но придется использовать комплексные числа:

$$x^2 + y^2 = (x + iy)(x - iy).$$

Определение 2.

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \tag{14}$$

называется *кольцом гауссовых чисел.*

Мы видим, что абстрактная алгебра появляется естественным образом из “классической” задачи.

Задача 12. Докажите, что $\mathbb{Z}[i]$ — подкольцо в $\mathbb{C}$, а $\mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$ — подполе в $\mathbb{C}$.

Определим норму гауссова числа $\alpha = x + iy$:

$$N\alpha = x^2 + y^2 = |\alpha|^2 = \alpha\bar{\alpha}. \tag{15}$$

Последняя формула показывает, что $N(\alpha\beta) = N\alpha \, N\beta$. Ясно, что целое число представимо в виде суммы двух квадратов если и только если оно является нормой некоторого гауссова числа.

Соглашение. Греческие буквы будут обозначать гауссовы числа, а латинские — целые числа.

Следствие 4.2. *Если числа m и n представимы в виде суммы двух квадратов, то и mn представимо в виде суммы двух квадратов.*

Задача 13. Докажите утверждение следствия, не используя гауссовы числа.

Простые целые числа — это числа, которые делятся только на 1 и на -1. Что является аналогом 1 и -1 в Гауссовых числах? Дадим общее определение.

Определение 3. Элемент ϵ кольца A называется *обратимым*, если найдется такой элемент ϵ', что $\epsilon\epsilon' = 1$.

Лемма 1. $\epsilon \in \mathbb{Z}[i]$ *обратим тогда и только тогда, когда* $N\epsilon = 1$.

Следствие 4.3. *Обратимые элементы кольца* $\mathbb{Z}[i]$ *суть* 1, -1, i *и* $-i$.

Задача 14. Пусть $D \in \mathbb{Z}$, $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Z}\}$. Найдите все обратимые элементы в $\mathbb{Z}[\sqrt{D}]$ при $D < 0$.

Замечание 3. Если $D > 0$ не является точным квадратом, то обратимые элементы кольца $\mathbb{Z}[\sqrt{D}]$ образуют группу, изоморфную $\mathbb{Z}$.

Назовем $\pi \in \mathbb{Z}[i]$ *разложимым*, если $\pi = \beta\gamma$, где β и γ необратимы. В противном случае назовем элемент *неразложимым.* Назовем элементы α и β *ассоциированными*, если $\alpha = \epsilon\beta$, где ϵ — обратим.

Задача 15. Отношение ассоциированности является отношением эквивалентности.

Теорема 5. *Каждое ненулевое гауссово число может быть записано в виде произведения неразложимых. Такое разложение единственно с точностью до перестановки множителей и замены неразложимых на ассоциированные.*

Доказательство аналогично доказательству для целых чисел, а именно, нужно воспользоваться следующим утверждением:

Задача 16 (Теорема о делении с остатком)**.** Пусть даны α и $\beta \neq 0$. Тогда найдутся такие ν и ρ, что $\alpha = \nu\beta + \rho$ и $N\rho < N\beta$.

Задача* 17. Докажите теорему об однозначности разложения.

Предостережение. Теорема об однозначности разложения чаще неверна, чем верна. Например, в $Z[\sqrt{-5}]$: $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

Задача 18. Докажите, что 3, 7, $1 + 2\sqrt{-5}$ и $1 - 2\sqrt{-5}$ неразложимы в $\mathbb{Z}[\sqrt{-5}]$.

Наша следующая цель, описать все неразложимые гауссовы числа.

Предложение 1.
(1) *Для любого* α *найдется целое число* a *такое, что* $\alpha | a$.
(2) *Для любого неразложимого* π *найдется простое целое число* p *такое, что* $\pi | p$. *В этом случае* $N\pi = p$ *или* $N\pi = p^2$. *(В этом случае говорят, что* π лежит над p.*)*
(3) *Обратно, пусть* p *— простое целое число. Если* p *не является нормой гауссово числа, то* p *неразложимо,* как гауссово число. *Если* $p = N\pi$, *то* $p = \pi\bar{\pi}$ *— разложение* p *на неразложимые гауссовы числа.*

Итак, осталось выяснить, какие простые целые разложимы в $\mathbb{Z}[i]$, а какие нет. На самом деле, нужно еще выяснить, не может ли быть так, что π и $\bar{\pi}$ ассоциированы.

Предложение 2. $2 = (1+i)(1-i) = -i(1+i)^2$. *Пусть $p > 2$ и $p = \pi\bar{\pi}$, тогда π и $\bar{\pi}$ не ассоциированы.*

Предложение 3. *p разложимо тогда и только тогда, когда $p = 4k+1$.*

Доказательство. Пусть p неразложимо и $p = 4k+1$. Тогда найдется такое m, что $p|m^2+1$ $\Big($например, ниже мы покажем, что можно взять $m = \left(\frac{p-1}{2}\right)!\Big)$. Но тогда $p|(m+i)(m-i)$. Будучи неразложимым, p делит $m+i$ или $m-i$. Но тогда $p|1$.

Осталось доказать, что

$$\left(\frac{p-1}{2}\right)^2 \equiv -1 \pmod p.$$

Сначала докажем, что $(p-1)! \equiv -1 \pmod p$. Действительно, остатки по модулю p, отличные от $-1 \equiv p-1$, разбиваются на пары обратных, поэтом их произведение равно -1. Но мы можем записать

$$(p-1)! \equiv \left(\frac{p-1}{2}\right)!(-1)(-2)\dots\left(-\frac{p-1}{2}\right).$$

Так как $p \equiv 1(\pmod 4)$, левая часть сравнима с $((p-1)/2)!$ по модулю p. □

Следующая теорема описывает все неразложимые гауссовы числа.

Теорема 6. *Пусть p — простое число.*

- *Если $p = 2$, то $1+i$ единственное неразложимое, лежащее над p, с точностью до ассоциированности, причем $2 = (1+i)(-i(1+i))$. Кроме того, $N(1+i) = 2$.*
- *Если $p \equiv 3 \pmod 4$, то p — единственное неразложимое гауссово число, лежащее над p, причем $Np = p^2$.*
- *Если $p \equiv 1 \pmod 4$, то найдется такое π, что $p = \pi\bar{\pi}$. При этом, с точностью до ассоциированности, над p лежит ровно два неразложимых: π и $\bar{\pi}$. Имеем $N\pi = N\bar{\pi} = p$.*

Задача 19. Пусть $n = p_1^{k_1}\dots p_l^{k_l}$ разложение числа n на простые множители. n представимо в виде суммы двух квадратов тогда и только тогда, когда для каждого p_i, такого, что $p_i \equiv 3 \pmod 4$, k_i четно.

2.2. **Дзета-функция гауссовых чисел.** Вернемся к Дзета-функции.

Определение 4.

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4} \sum_{\alpha \in \mathbb{Z}[i], \alpha \neq 0} \frac{1}{N\alpha^s}. \tag{16}$$

Ясно, что

$$\zeta_{\mathbb{Z}[i]}(s) = \sum_{(a,b) \neq (0,0)} \frac{1}{(a^2+b^2)^s}. \tag{17}$$

Мы можем переписать $\zeta_{\mathbb{Z}[i]}(s)$ в виде ряда Дирихле

$$\sum_{n=1}^{\infty} \frac{q_n}{n^s}, \tag{18}$$

где q_n — число представлений n в виде суммы квадратов двух неотрицательных чисел. Этот ряд сходится при $s > 1$.

Теорема 7.

$$\zeta_{\mathbb{Z}[i]}(s) = \prod_{\pi} \left(1 - \frac{1}{N\pi^s}\right)^{-1}, \tag{19}$$

где в произведении участвует по одному неразложимому из каждого класса ассоциированности.

Для $p \equiv 1 \pmod 4$ обозначим через π_p какое-нибудь гауссово число с нормой p. Имеем

$$\zeta_{\mathbb{Z}[i]}(s) = \tag{20}$$

$$\left(1 - \frac{1}{N(1+i)^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{N\pi_p^s}\right)^{-1} \left(1 - \frac{1}{N\bar{\pi}_p^s}\right)^{-1} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{Np^s}\right)^{-1} =$$

$$\left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^{2s}}\right)^{-1} =$$

$$\zeta(s) \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 3 \pmod 4} \left(1 + \frac{1}{p^s}\right)^{-1}.$$

Определим $\chi : \mathbb{Z} \to \{-1, 0, 1\}$ так: $\chi(2k) = 0$, $\chi(4k+1) = 1$, $\chi(4k+3) = -1$. Определим *L-функцию*:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{21}$$

2.2.1. *L-функции Дирихле.* Сделаем небольшое отступление. Пусть $\chi : \mathbb{Z} \to \mathbb{C}$ — функция, обладающая следующим свойством:

$$\chi(mn) = \chi(m)\chi(n) \text{ для любых } m \text{ и } n. \tag{22}$$

Обозначим ряд Дирихле $\sum \frac{\chi(n)}{n^s}$ через $L(s, \chi)$

Задача 20. Придумайте аналог произведения Эйлера для ряда Дирихле $L(s, \chi)$. А что можно сказать, если свойство (22) выполняется только для взаимно-простых m и n?

Замечание 4. Пусть функция χ обладает свойством (22) и еще следующим свойством: существует N такое, что $\chi(n) = \chi(n + N)$ при всех n и $\chi(n) \neq 0$ тогда и только тогда, когда n и N взаимно-просты. Тогда χ называется *характером Дирихле*, а $L(s, \chi)$ называется *L-функцией Дирихле.*

2.2.2. *Окончание вывода формулы для числа представлений в виде суммы квадратов.* Из этой задачи следует, что

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Итак

$$\zeta_{\mathbb{Z}[i]}(s) = \zeta(s)L(s, \chi) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} \chi(d)}{n^s}.$$

Следствие 7.1. *Число представлений n в виде суммы квадратов двух неотрицательных целых чисел равно разности числа положительных делителей вида $4k + 1$ и числа делителей вида $4k + 3$.*

2.3. **Обобщение.** Все вышесказанное верно (с минимальными изменениями) для $\mathbb{Z}[\sqrt{-D}]$, если выполняется теорема об однозначном разложении. К сожалению, выполняется она редко (для положительного D только при $D = 1, 2, 67$.)

Задача* 21. Докажите, что $\mathbb{Z}[\sqrt{-2}]$ обладает однозначностью разложения и выясните какие числа представляются в виде $a^2 + 2b^2$.

На следующем занятии мы объясним, что всегда имеется некоторый аналог однозначности разложения. Но сначала мы хотим расширить класс колец, с которыми мы работаем.

3. Занятие 3. Дзета-функция Дедекинда, локальная Дзета-функция

На этом занятии мы будем изучать обобщения Дзета-функции кольца гауссовых чисел на другие квадратичные кольца и более общие числовые поля. В конце занятия мы займемся обобщением на высшие размерности.

3.1. **Целозамкнутые числовые кольца. Однозначность разложения.** Мы будем изучать следующий класс колец:

Определение 5. $A \subset \bar{\mathbb{Z}}$ называется *числовым кольцом*, если оно порождается конечным числом целых алгебраических чисел.

Примеры: $\mathbb{Z}[\sqrt{D}]$, $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$, $\mathbb{Z}[\sqrt[3]{2}]$.

Нам понадобится следующее техническое условие на A. Рассмотрим поле частных $QA = \{a/b|a, b \in A\}$. Ясно, что QA подполе в $\mathbb{Q}$. Кольцо A называется *целозамкнутым*, если $QA \cap \bar{\mathbb{Z}} = A$. Мы будем предполагать, что A целозамкнуто.

Пример 1. Кольцо $\mathbb{Z}[\sqrt{-3}]$ не целозамкнуто.

Замечание 5. С геометрической точки зрения, целозамкнутость — это свойство, похожее на гладкость (точнее более слабое). Если A не целозамкнуто, то можно заменить его на $QA \cap \bar{\mathbb{Z}}$, которое уже обязательно будет целозамкнутым.

Задача 22. Пусть $A \subset \bar{\mathbb{Z}}$ порождено конечным числом целых алгебраических чисел, и в A выполняется однозначность разложения на множители. Тогда A целозамкнуто.

Задача 23. При каких D $\mathbb{Z}[\sqrt{D}]$ целозамкнуто?

Вернемся к идеалам.

Определение 6. Пусть A кольцо (ассоциативное, коммутативное с единицей), тогда $\mathfrak{a} \subset A$ называется *идеалом*, если для любых $a, b \in \mathfrak{a}$ имеем $a + b \in \mathfrak{a}$ и для любых $a \in \mathfrak{a}$, $b \in A$ имеем $ab \in \mathfrak{a}$.

Задача 24. Для любого $a \in A$ множество $(a) = aA = \{ab|b \in A\}$ является идеалом. (Такой идеал называется *главным.*)

Целостное кольцо, в котором все идеалы главные, называется *областью главных идеалов.*

Задача 25. $\mathbb{Z}$, $\mathbb{Z}[i]$, $k[x]$ области главных идеалов. (Указание: рассмотрите элемент идеала с наименьшей нормой.)

Задача* 26. Докажите, что в области главных идеалов каждый ненулевой элемент разлагается на множители однозначно с точностью до замены на ассоциированные.

Задача 27. $(a) = A$ тогда и только тогда, когда a обратим. $(a) = (b)$ тогда и только тогда, когда a и b ассоциированы. $(a) \supset (b)$ тогда и только тогда, когда a делит b.

Для идеалов $\mathfrak{a}$ и $\mathfrak{b}$ определим идеал $\mathfrak{ab} = \{a_1b_1 + \ldots + a_kb_k|a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. Ясно, что $(a)(b) = (ab)$. Заметим, что $\mathfrak{a} \supset \mathfrak{ab}$.

Напомним, что идеал $\mathfrak{p} \neq A$ *прост*, если $ab \in \mathfrak{p}$ влечет $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Ясно, что $(p) \in \mathbb{Z}$ прост тогда и только тогда, когда p простое число.

Факт 3. *Каждый ненулевой идеал в A однозначно разлагается в произведение простых. Идеал $\mathfrak{p}$ неразложим тогда и только тогда, когда он прост. Идеал $\mathfrak{a}$ делит идеал $\mathfrak{b}$, тогда и только тогда, когда $\mathfrak{a} \supset \mathfrak{b}$.*

Задача 28. Докажите этот факт для $\mathbb{Z}$ и $\mathbb{Z}[i]$. Указание: замена a на ассоциированный не меняет (a).

Задача 29. В $\mathbb{Z}[\sqrt{-5}]$ имеем $(3) = (3, 1 + 2\sqrt{-5})(3, 1 - 2\sqrt{-5})$.

Будем писать $a \equiv b \pmod{\mathfrak{a}}$, если $a - b \in \mathfrak{a}$. Обозначим через $A/\mathfrak{a}$ множество классов эквивалентности. Напомним, что это множество является кольцом.

Предложение 4. *Если $\mathfrak{a} \neq (0)$, то $A/\mathfrak{a}$ конечно.*

Доказательство. Каждый ненулевой идеал содержит ненулевое целое число. □

Число элементов в $A/\mathfrak{a}$ называется *нормой идеала*. Обозначение $N\mathfrak{a}$.

Факт 4. $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}\, N\mathfrak{b}$.

Задача 30. Пусть $\alpha \in \mathbb{Z}[i]$, тогда $N(\alpha) = N\alpha$. Указание: Используйте два предыдущих факта.

3.2. **Идеалы, лежащие над простым числом p.**

Мы хотим получить аналог теоремы, описывающей простые гауссовы числа в более общей ситуации.

Предложение 5. *Каждый ненулевой простой идеал содержит единственное простое число p.*

Рассмотрим *редукцию по модулю p* — факторкольцо A/pA. Напомни, см. Дополнение), что Имеется взаимно однозначное соответствие между простыми идеалами в A, лежащими над p, и простыми идеалами в A/pA и

Предположим, что наше кольцо A порождено единственным $\alpha \in \bar{\mathbb{Z}}$. Тогда $A = \mathbb{Z}[\alpha] \approx \mathbb{Z}[x]/(g(x))$, где $g(x)$ — минимальный многочлен α.

Пусть p — целое простое число. Имеем

$$A/pA = \mathbb{Z}[x]/(p, g(x)) = \mathbb{F}_p[x]/\bar{g}(x)\mathbb{F}_p[x],$$

где $\bar{g}$ редукция g по модулю p.

Напомним, что для любого n существует единственное с точностью до изоморфизма поле из p^n элементов. Более того, пусть $\bar{\mathbb{F}}_p$ фиксированное алгебраическое замыкание поля $\mathbb{F}_p$, тогда $\bar{\mathbb{F}}_p$ содержит единственное подполе из p^n элементов, которое мы обозначим через $\mathbb{F}_{p^n}$, причем $\bar{\mathbb{F}}_p = \cup_{n=1}^{\infty}\mathbb{F}_{p^n}$. Кроме того, $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ тогда и только тогда, когда $n|m$.

Рассмотрим разложение g на неприводимые в $\mathbb{F}_p[x]$:

$$\bar{g}(x) = h_1(x)h_2(x)\dots h_k(x). \tag{23}$$

Говорят, что A *разветвлено* в p, если среди этих множителей есть одинаковые.

Лемма 2. *Разложим $\bar{g}$ в произведение линейных множителей в $\bar{\mathbb{F}}_p[x]$:*

$$\bar{g}(x) = (x-\alpha_1)\dots(x-\alpha_{\deg g}). \tag{24}$$

A разветвлено в p если и только если среди этих множителей есть одинаковые.

Предложение 6. *A разветвлено лишь в конечном числе простых чисел.*

Доказательство. Докажем для g степени 2. Если $\mathbb{Z}[x]/(x^2+bx+c)$ разветвлено в p, то $p|b^2-4ac$. □

Задача 31. В каких простых разветвлены $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-D}]$, $\mathbb{Z}[\sqrt[3]{2}]$?

Пусть A не разветвлено в p.

Теорема 8. *Пусть $\deg h_j = f_j$, тогда*
(a)

$$A/pA \approx \prod_{j=1}^{k} \mathbb{F}_{p^{f_j}}.$$

(b) В A/pA ровно k простых идеалов:

$$\mathfrak{p}_j = \prod_{j\neq l} \mathbb{F}_{p^{f_l}},$$

причем $N\pi^{-1}(\mathfrak{p}_j) = p^{f_j}$.

Следствие 8.1. *Пусть q и p — простые числа, $q \equiv 3 \pmod 4$. Идеал (p) разложим в $\mathbb{Z}[\sqrt{-q}]$ если и только если уравнение $x^2 = -q$ имеет решение в $\mathbb{F}_p$.*

3.3. **Дзета-функция.** Определим *Дзета-функцию Дедекинда*:

$$\zeta_A(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}, \tag{25}$$

где произведение берется по ненулевым простым идеалам. Имеем

$$\zeta_A(s) = \sum_{n=1}^{\infty} a_n n^s, \tag{26}$$

где a_n — число идеалов с нормой n.

Предложение 7. *Если $q \equiv 1 \pmod 4$, то*

$$\zeta_{\mathbb{Z}[\sqrt{-q}]}(s) = \zeta(s)L(s,\chi),$$

где мультипликативный характер $\chi : \mathbb{Z} \to \{-1,0,1\}$ определен так: $\chi(q) = 0$, $\chi(2) = 0$, $\chi(p) = \pm 1$ в зависимости от того, имеет ли сравнение $x^2 \equiv -q \pmod p$ решение.

Задача* 32. Вычислите $\zeta_{\mathbb{Z}[\sqrt{D}]}$ в общем случае.

Мы можем переписать

$$\zeta_A(s) = \prod_p \prod_{p \in \mathfrak{p}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1} = \prod_p \prod_j (1 - p^{-f_j(p)s})^{-1}.$$

Ясно, что множитель, соответствующий p, — рациональная функция от p^{-s}, которую мы назовем *локальной Дзета-функцией*:

$$Z_{A/pA}(t) = \prod_j (1 - t^{f_j})^{-1} = \prod_l (1 - t^l)^{-_l},$$

где $_l$ число многочленов h_j, имеющих степень l. Иными словами:

$$\zeta_A(s) = \prod_p Z_{A/pA}(p^{-s}). \tag{27}$$

3.4. **Локальная Дзета-функция.** Вернемся к фиксированному p. Запишем

$$\bar{g} = (x - \alpha_1) \dots (x - \alpha_{\deg g}).$$

Обозначим через N_k количество α_j, лежащих в $\mathbb{F}_{p^k}$, то есть число решений уравнения $g(x) = 0$ в $\mathbb{F}_{p^k}$. (Напомним, что $\bar{\mathbb{F}} = \cup_k \mathbb{F}_{p^k}$.) Имеем

$$N_k = \sum_{l|k} l c_l.$$

Это следует из такого утверждения: Если α — корень $h_j(x)$, то $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^{\deg g_j}}$.

Мы хотим выразить $Z_{A/pA}(t)$ в терминах N_k. Пусть $Y_{A/pA}(t) = \sum_{k=1}^{\infty} N_k t^{k-1}$.

Предложение 8.

$$Z_{A/pA}(t) = \exp\left(\int Y_{A/pA}(t)\right) = \exp\left(\sum_k \frac{N_k}{k} t^k\right), \qquad Y_{A/pA}(t) = Z'_{A/pA}(t)/Z_{A/pA}(t).$$

Задача 33. Докажите, что Z рациональная функция тогда и только тогда, когда Y рациональна, степень числителя не превосходит степени знаменателя и Y не имеет кратных корней и/или полюсов.

4. Занятие 4. Формула для числа классов, “гипотезы” Вейля, гипотеза Берча и Свиннертон-Дайера

Все нижеследующее надо понимать в таком ключе: Дзета-функция несет информацию о важных инвариантах соответствующей системы уравнений. Оказывается, например, что из Дзета-функции Дедекинда можно извлечь интересную информацию о числовом поле.

4.1. **Формула для числа классов.** Назовем идеалы $\mathfrak{a}, \mathfrak{b} \subset A$ *эквивалентными по модулю главных идеалов*, если найдутся такие $a, b \in A \setminus 0$, что $(a)\mathfrak{b} = (b)\mathfrak{a}$. Обозначим число классов эквивалентности через h. Оказывается, h всегда конечно. Оно называется *числом классов кольца* A. В частности A — область главных идеалов тогда и только тогда, когда $h = 1$.

Факт 5. *Для* $\mathbb{Z}[\sqrt{-q}]$, *где* $q < 0$ *свободно от квадратов и* $q \not\equiv 3 \pmod 4$*:*

$$\lim_{s \to 1}(s-1)\zeta_{\mathbb{Z}[\sqrt{-q}]}(s) = \frac{\pi h}{w\sqrt{q}},$$

где w *— число обратимых элементов.*

Заметим, что в левой части стоит неопределенность типа $0 \cdot \infty$. Ее предел называется *вычетом.*

Задача* **34.** Докажите этот факт.

Задача 35. Выведите из этого факта, что разложение на множители в $\mathbb{Z}[i]$ однозначно. Указание: Проверьте, что для соответствующей L-функции $L(1, \chi) = \pi/4$.

4.2. **Напоминание.** Напомним наш основной результат об идеалах, лежащих над p.

Пусть $A = \mathbb{Z}[\alpha] \approx \mathbb{Z}[x]/(g(x))$, где $g(x)$ — минимальный многочлен α. Пусть p — целое простое число. Имеем

$$A/pA = \mathbb{Z}[x]/(p, g(x)) = \mathbb{F}_p[x]/\bar{g}(x)\mathbb{F}_p[x],$$

где $\bar{g}$ редукция g по модулю p. Рассмотрим разложение g на неприводимые в $\mathbb{F}_p[x]$:

$$\bar{g}(x) = h_1(x)h_2(x)\dots h_k(x). \tag{28}$$

Пусть A неразветвлено в p, то есть все множители различны. Напомним, что простые в A, лежащие над p находятся в биективном соответствии с $h_i(x)$, причем норма соответствующего идеала равна

$$p^{\deg h_i} = p^{f_j(p)},$$

(мы обозначили степень h_i через $f_j(p)$.)

4.3. **Многомерный случай.** Пусть $I = (g_1, \dots, g_n)$ — идеал в $\mathbb{F}_p[x_1, \dots, x_m]$. Положим $B = \mathbb{F}_p[x_1, \dots, x_m]/I$. I определяет *алгебраическое множество*

$$\bar{V} = \{x \in \bar{\mathbb{F}}_p^m | g_1(x) = \dots g_n(x) = 0\}.$$

Обозначим

$$V_k = \bar{V} \cap \mathbb{F}_{p^k}^m.$$

Ясно, что V_k конечно. Выше мы рассматривали случай $m = 1$, $I = (g(x))$. В этом случае не только V_k, но и $\bar{V}$ были конечными.

Пусть $N_k = |V_k|$. По аналогии с предыдущим определим *локальную Дзета-функцию*

$$Z_B(t) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k t^k}{k}\right). \tag{29}$$

Можно показать, что $Z_B(t)$ зависит только от B.

Пример 2. Если I — система линейных уравнений, то

$$Z_B(t) = \frac{1}{1-p^d t},$$

где $d = \dim \bar{V} = m - \operatorname{rk} I$.

Задача 36. Если $m = 2$, $I = (x^2 - y^2 - 1)$, то

$$Z_B(t) = \frac{1-t}{1-pt}.$$

Задача 37. Вычислите локальную Дзета-функцию для $\mathbb{F}_p[x, y, z, t]/(x^2 + y^2 - z^2 - t^2)$.

Наконец, пусть $J = (h_1, \dots, h_n)$ идеал в $\mathbb{Z}[x_1, \dots, x_m]$. Положим $A = \mathbb{Z}[x_1, \dots, x_m]/J$, определим *Дзета-функцию Хассе–Вейля* формулой

$$\zeta_A(s) = \prod_p Z_{A/pA}(p^{-s}). \tag{30}$$

Замечание 6. На самом деле, множители, соответствующие тем p, для которых редукция задает *особое* многообразие (см. ниже), неправильны. К счастью, таких p — конечное число (аналогично ситуации с ветвлением). Поэтому следует считать, что эта функция определена лишь с точностью до конечного числа множителей.

4.4. **Гипотезы Вейля для плоских кривых.** Проективная плоскость $\mathbb{P}^2_{\mathbb{F}}$ определяется как множество наборов $(X : Y : Z)$, где $(X, Y, Z) \neq (0, 0, 0)$ и наборы, получающиеся друг из друга умножением на ненулевой скаляр считаются эквивалентными. Иначе говоря, $\mathbb{P}^2_{\mathbb{F}}$ — множество прямых в $\mathbb{F}^3$. Имеем

$$\mathbb{P}^3_{\mathbb{F}} = \mathbb{F}^2 \sqcup \mathbb{P}^1_{\mathbb{F}} = \mathbb{F}^2 \sqcup \mathbb{F}^1 \sqcup \mathbb{F}^0.$$

Пример 3. Две квадрики в $\mathbb{P}^2_{\mathbb{C}}$ пересекаются ровно в четырех точках или имеют общую компоненту, если точки пересечения считать с кратностями. Это утверждение не верно, ни в $\mathbb{P}^2_{\mathbb{R}}$, ни в $\mathbb{C}^2$.

Уравнение $F(X, Y, Z) = 0$ задает некоторое множество в $\mathbb{P}^2_{\bar{\mathbb{F}}}$, если оно *однородно.* Такое множество называется *кривой.* Например, $x^2+y^2 = 1$ есть пересечение $X^2 + Y^2 = Z^2$ с $\mathbb{F}^2$.

Кривая называется *гладкой*, если система

$$\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = \frac{\partial f}{\partial Z} = f = 0$$

не имеет ненулевых решений в $\mathbb{P}^2_{\bar{\mathbb{F}}}$. Итак, пусть $f \in \mathbb{F}_p[Z, Y, Z] = 0$, $f(X, Y, Z) = 0$ — гладкая кривая. Мы можем определить $Z_f(t)$ формулой (29). Оказывается

$$Z_f(t) = \frac{P(t)}{(1-t)(1-pt)}, \tag{31}$$

где $P(t)$ многочлен, $P(0) = 1$ и все корни многочлена $P(t)$ имеют модуль $1/\sqrt{p}$.

Рассмотрим теперь глобальную ситуацию. Пусть $f(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$. Многочлен f также задает кривую C в $\mathbb{P}^2_{\mathbb{C}}$. Предположим, что эта кривая гладкая, тогда топологически она представляет собой сферу с g ручками. Можно показать, что в нашем случае $g = (\deg f - 1)(\deg f - 2)/2$.

С другой стороны, пусть $f_p \in \mathbb{F}_p[X, Y, Z]$ — редукция f по модулю p, $P_p(t)$ — многочлен из (31). Оказывается (для почти всех p) $\deg P(t) = 2g$.

Аналогичное утверждение верно и для неплоских кривых, и в высших размерностях.

Задача 38. Проверьте гипотезы Вейля для случая $\deg f = 1$.

Задача 39. Вычислите Дзета-функцию для $X^2 + Y^2 = Z^2$. Проверьте гипотезы Вейля в этом случае. Вычислите Дзета-функцию для аффинной кривой $x^2 + y^2 = 1$.

Пример. Если $\deg f = 3$, то $g = 1$ и $P(t) = 1 - at + pt^2$.

4.5. **Гипотеза Берча и Свиннертон-Дайера.**

Факт 6. *При $g = 0$ уравнение $f(X, Y, Z) = 0$ имеет нулевое или бесконечное число решений в $\mathbb{P}^2_{\mathbb{Q}}$. При $g > 1$ это множество решений конечно. При $g = 1$ это множество представляет собой* абелеву группу конечного ранга.

При $g = 1$ кривая называется *эллиптической*, а ранг группы рациональных точек называется ее рангом.

Имеем (для почти всех p):

$$Z_{f_p}(t) = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)}.$$

Задача 40. Выразите число решений уравнения $f(X, Y, Z) = 0$ в $\mathbb{P}^2_{\mathbb{F}_{p^k}}$ через a_p.

Рассмотрим глобальную Дзета-функцию кривой E:

$$\zeta_f(s) = \prod_p Z_{f_p}(p^{-s}) = \prod_p \frac{1 - a_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} = \frac{\zeta(s)\zeta(s-1)}{L(f,s)}.$$

Напомним, что *порядок нуля* аналитической функции $\phi(z)$ в точке a это единственное целое число k такое что $\phi(z) = (z-a)^k \psi(z)$, где $\psi(a) \neq 0$.

Гипотеза Берча и Свиннертон-Дайера. Пусть f задает эллиптическую кривую. Тогда порядок нуля $L(f,s)$ в $s=1$ равен ее рангу. В частности число рациональных точек конечно тогда и только тогда, когда $L(f,1) \neq 0$.

5. Приложение: Комплексный анализ

Теорема 9. *Пусть f и g голоморфные функции на* связном *открытом множестве U. Пусть $A = \{z \in U : f(z) = g(z)\}$. Если Множество A имеет предельную точку, то функции f и g совпадают на U.*

Набросок доказательства. Пусть $h = f - g$, тогда h обращается в ноль на A. По условию мы можем выбрать последовательность различных точек $z_n \in A$ так, чтобы $\lim_{n\to\infty} z_n \in A$. Обозначим этот предел через z. Так как функция аналитична, мы можем разложить ее в ряд (13) в окрестности точки z. Пусть этот ряд ненулевой. Пусть a_k — первый ненулевой коэффициент ряда, тогда

$$f(w) = a_k(w-z)^k(1 + b_1(w-z) + b_2(w-z)^2 + \ldots).$$

Так как $f(z_n) = 0$, второй множитель обращается в ноль в z_n. Но тогда, по соображениям непрерывности, он обращается в ноль и в z. Это противоречие показывает, что наш ряд нулевой, а значит, функция нулевая в окрестности точки z.

Обозначим через B множество таких точек $z \in U$, что f обращается в нуль в окрестности z. Мы доказали, что B не пусто. Из предыдущего рассуждения также следует, что это множество замкнуто. Но оно, очевидно, открыто. Так как U связно, получаем $U = B$. □

6. Дополнение: Алгебра

Теорема 10. *Имеется взаимно однозначное соответствие между простыми идеалами в A, лежащими над p, и простыми идеалами в A/pA.*

Доказательство. Рассмотрим отображение $\pi : A \to A/pA$. Для идеала $\mathfrak{p} \subset A/pA$ рассмотрим идеал $\pi^{-1}(\mathfrak{p})$. Отображение $\mathfrak{p} \mapsto \pi^{-1}(\mathfrak{p})$ задает искомую биекцию. □